# How the FBI hacked El Chapo's encrypted phone network

Keegan Hamilton ⋮ 7-9 minutes ⋮ 1/9/2019

*Listen to **"Chapo: Kingpin on Trial"** for free, exclusively on Spotify.*

Joaquín "El Chapo" Guzmán had it all figured out. Sometime in the late 2000s, he hired a systems engineer to design an encrypted communications network for the Sinaloa cartel. The system was supposed to let him discuss business on the phone without worrying about eavesdropping by law enforcement. That system worked as intended for years — right up until the engineer became an informant for the FBI.

## Videos by VICE

Chapo's trial just entered its third month, and some of the most jaw-dropping testimony yet came Tuesday when FBI special agent Stephen Marston described how U.S. federal agents cracked the Sinaloa cartel's encrypted phone network by recruiting the man who created it. Marston narrated as federal prosecutors played multiple recordings of calls featuring El Chapo's voice, offering jurors an unfiltered view of how the kingpin ran his organization.

In the calls, Chapo can be heard micromanaging his cartel's day-to-day operations, with each recording seeming more incriminating than the one before. Chapo asks his underling to hand the phone over to a corrupt police commander so that he can personally request a "special favor." He warns his enforcer not to "execute innocent people" during a conflict with a rival group. Chapo persuades a client looking to distribute cocaine in Ohio to accept a shipment of meth instead. Marston testified that the FBI has recordings of over 800 such calls made by Sinaloa cartel members, up to 200 of which include Chapo's voice.

Marston said in 2009 the FBI began investigating Cristián Rodriguez, the suspected architect of a "secure communication system" used by Jorge Cifuentes, a Colombian cocaine kingpin who testified against Chapo last month. Cifuentes told the jury that he recommended Rodriguez to Chapo and sent him to the mountains of Sinaloa to set up a wireless internet network and design a custom network that offered "secure communications."

According to Marston, the system proved to be impenetrable. The FBI had gained access to devices that Sinaloa cartel members used to communicate with each on the network. But the encryption, which required special keys to unlock, proved too difficult to break without help.

On Feb. 3, 2010, the FBI lured Rodriguez to a hotel in Manhattan by posing as members of a Russian mafia group who wanted to pay for his services. "We realized that without insider access to the system, we were not going to get inside," Marston said.

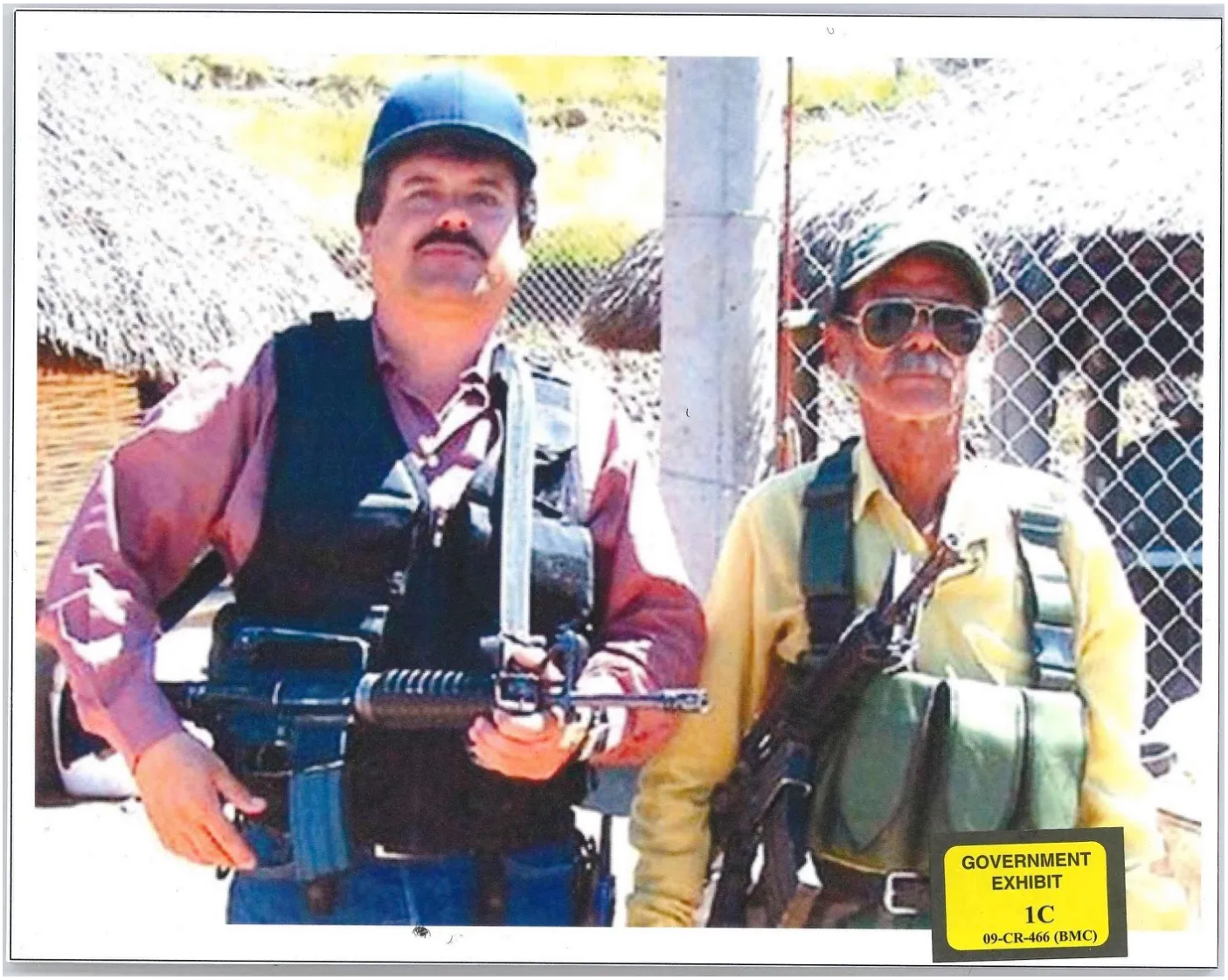


Photo via the U.S. Attorney's Office.

Rodriguez eventually agreed to "proactively cooperate" with the FBI starting in early 2011. He relocated three servers that he'd set up to host the cartel's encrypted network from Canada to the Netherlands, passing off the move as part of a routine upgrade. The FBI had enlisted Dutch authorities to help with the investigation, and they were soon able to listen in as Chapo, oblivious to the betrayal, spoke freely with his most trusted associates.

In one call recorded early in the morning on April 9, 2011, Chapo speaks with Orso Iván Gastélum Cruz (aka Cholo Iván), a feared cartel hitman, about issues they had been having with police in Sinaloa. Cholo brags about beating up the cops, but Chapo warns that it will only cause problems.

"Don't be so harsh, fucking Cholo. Take it easy with the police," Chapo says.

"Well, you taught us to be a wolf, acting like a wolf," Cholo responds. "I'm remembering and that is how I like to do it."

Marston explained that the network Rodriguez designed for the Sinaloa cartel used Voice Over Internet Protocol, or VoIP, similar to Skype or Google Voice, and it required users to access the internet. Two of the Dutch servers were used for phone calls, and a third was reserved for text messages, though Marston said Chapo never sent any.

According to Marston, Rodriguez's system allowed users to make two types of phone calls. He compared one to a closed phone network at a corporate office, where users could reach each other by dialing a three-digit extension. (The FBI would later recover a makeshift phonebook with extension listings for various cartel members from a home where Chapo was hiding out in Cabo San Lucas.) The other type of call required users to essentially dial out of the network and enter a conventional phone number. All of the calls were outgoing — there was no way for an outsider to reach a cartel member on the network.

Marston said there were technical difficulties that initially prevented the FBI from receiving all of the data from the calls, or caused them to receive calls that were still protected by encryption. And once the FBI had unfettered access, the agents had to verify that it was actually Chapo's voice on the line. Chapo inadvertently helped with that task by supplying samples of voice for comparison — his videotaped interview with Rolling Stone in 2016, along with calls he made last year from his federal jail in Manhattan.

"In general, it has a higher pitch," Marston said, describing Chapo's voice. "It has kind of a sing-songy nature to it, and I pick up kind of a nasally undertone."

***Listen to the real story behind the rise — and trial — of a kingpin.***

Marston testified that Chapo gradually stopped using the encrypted network and abandoned it entirely by the end of 2011. It may have had something to do with reliability. Several recordings played in court ended abruptly when Chapo or the other caller lost signal. Cifuentes also complained during his testimony that Rodriguez was "an irresponsible person," who forgot to renew the license on the software they had purchased.

When Cifuentes testified, prosecutors played several calls for the jury, including a conversation where Chapo can be heard negotiating the purchase of eight tons of cocaine from FARC guerrillas in Colombia. Cifuentes said he believed U.S. authorities were able to obtain the calls only because he and Chapo were using conventional phones while the encrypted network was down — not because Rodriguez was working for the FBI.

Rodriguez is also expected to testify against Chapo, potentially as soon as Wednesday. Federal prosecutors have moved to block Chapo's lawyers from asking a witness, believed to be Rodriguez, about mental health issues caused by "the stress associated with his work" for Chapo, along with "his cooperation with the U.S. government."

It's still unclear whether Rodriguez helped U.S. authorities pinpoint Chapo's location and ultimately capture him, but DEA agents have previously disclosed that they tracked Chapo in part through his use of encrypted BlackBerry cellphones. Rodriguez continued working for the FBI until 2013, and he apparently still fears for his life. Prosecutors successfully petitioned the judge to prevent courtroom sketch artists from drawing Rodriguez's face for fear the cartel could use the images to track him down. A photo of Rodriguez was shown in court Tuesday, but it was pixelated when released to the media.

*Cover: A government exhibit, via the U.S. Attorney's Office.*